IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 October 2023, accepted 19 October 2023, date of publication 30 October 2023, date of current version 3 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3328569

RESEARCH ARTICLE

Enhancing Supply Chain Efficiency and Security: A Proof of Concept for IoT Device Integration With Blockchain

YASH MADHWAL[1], (Member, IEEE), YURY YANOVICH[1], (Member, IEEE), S. BALACHANDER[2], K. HARSHINI POOJAA[2], R. SARANYA[2], AND B. SUBASHINI[2]

[1]Center for Next Generation Wireless Technologies and IoT, Skolkovo Institute of Science and Technology, 121205 Moscow, Russia
[2]Department of Data Science and Business Systems, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu 603203, India

Corresponding author: Yash Madhwal (yash.madhwal@skoltech.ru)

ABSTRACT The manufacturing industry comprises various departments, and the supply chain is crucial in ensuring uninterrupted commodity flow during production. However, traditional supply chain systems face transparency, data visibility, and security challenges. This scientific article presents a Proof of Concept (PoC) that explores integrating IoT devices with blockchain technology to address these issues. Our PoC focuses on enabling IoT devices to autonomously sign transactions to the blockchain using IoT devices' authenticated private keys, eliminating the need for external wallets. This approach offers scalability, efficiency, and real-time responsiveness benefits. Leveraging the devices' transaction processing capabilities enhances scalability, allowing for a higher transaction volume. Automation of transaction signing streamlines the process, improving efficiency and eliminating delays caused by human interaction. Real-time responsiveness is ensured, eliminating any latency introduced by external wallets. We provide a detailed workflow of the use case and simulation results, making our research findings more accessible. Through this work, we demonstrate the feasibility and advantages of this method in scenarios where continuous, automated interaction with the blockchain is required through IoT devices. The PoC code is publicly available on GitHub.

INDEX TERMS Accessibility, blockchain, Internet of Things (IoT) devices, real-time responsiveness, supply chain management.

I. INTRODUCTION

The manufacturing industry is divided into four main departments: sales and marketing, information technology and finance, supply chain management, and research and development. The supply chain, however, serves as the foundation of enterprises since it ensures the continuous flow of commodities throughout the production process. The phrase ‘‘supply chain'' is more comprehensive, including cross-departmental communication and back-and-forth between suppliers and clients [1]. It may be used to define every process step, from raw materials to final products with added value, including post-sale support, logistical challenges, and reversal logistics. These procedures include need and supply planning, forecasting, production, and product delivery [2].

Even while many big businesses have transitioned to IT-based technical infrastructures from utilizing physical ledgers, electronic mail, and spreadsheets, the main difficulty of ensuring that goods flow properly and can be scrutinized at every level has not been resolved [3]. Since these technologies use centralized database management systems, they are also subjected to tampering and safety risks. Another problem with these systems is that none of the stakeholders in the supply chain have relationships or data visibility. For instance, the extension of the supply chain system due to factors like globalization and increased intermediaries between producers and consumers has decreased transparency concerning product origins and shipping information [4].

Transporting hazardous materials and other items requires special precautions to protect human health and the natural

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Arafatur Rahman.

© 2023 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

environment [5]. This is a descriptive and scientific issue. Poor business results have been attributed to a lack of communication among supply chain partners [6]. The current supply chain and transportation challenges may be summed up in one phrase a dearth of trustworthy data and data visibility. It is crucial to manage the material movement across all of the participants in a supply chain with the necessary transparency and dependability because of the complex nature of the chain itself. Accurate demand and stock projections, scheduling of materials and manufacturing, and better inventory management rely heavily on this information [7].

The COVID-19 pandemic highlighted the supply chain's vulnerability. The semiconductor shortage, once a small inconvenience, has become a worldwide problem affecting consumer goods, motor vehicles, healthcare devices, electricity, and practically all industries. It highlighted the frail supply chain networks of several huge, well-established enterprises. Any big supply chain interruption may derail an organization and hurt revenue and profitability. The supply chain network collapse impacted organization of all sizes, sectors, and locations, revealing their inefficient procedures. Even well-known enterprises lack reliable supply chain data [8]. For large corporations that employ a variety of global vendors and suppliers to reduce manufacturing costs, transparency and integrity are essential.

The expansion of commodities and the global network of suppliers has increased the production chain's complexity and the logistics chain's length, leading to many points of failure [9]. This made businesses recognize how important it was to digitize their supply chains and transportation infrastructure and to use cutting-edge technologies like blockchain and the Internet of Things (IoT) to improve data security and visibility. Modern systems can swiftly respond to unanticipated events based on real-time monitoring of transport parameters using sensors. While sensor data may be helpful, proof will still be required to back up security claims, and costs will need to be expended just as with any other liability insurance [10]. Promoting data privacy and integrity while encouraging interoperability across technologies and stakeholders is essential. Updating infrastructure, integrating old systems, and adhering to regulations are difficult but necessary jobs. To achieve success, all key stakeholders must collaborate efficiently [11].

For logistics, which is the science and technology of administering all kinds of processes (materials, knowledge, funds, and activities), Blockchain is a tool for a certain kind of digital business management. With this description, IoT possibilities, and smart goals, a fresh wave of systems and technology for operations and the supply chain could be made in the future [12], [13].

The external wallet is essential for signing transactions and interacting with the blockchain. It offers an extra layer of security by keeping private keys separate from online platforms and applications, decreasing the risk of unauthorized access to confidential information [14]. When users start a transaction, their external wallet is secure storage for their private keys [15]. The user's wallet software generates the transaction and signs it with the private key linked to their account. Afterward, the signed transaction is sent to the blockchain network for validation and inclusion in the ledger [16]. However, it is imperative to note that external wallets require human interaction to confirm transactions. This manual confirmation process can introduce significant delays, as it relies on individuals to review and authorize each transaction [17]. This poses a significant challenge in the context of IoT devices, which are designed for autonomous operation, as they cannot seamlessly integrate with external wallets that necessitate human confirmation. IoT devices are often programmed to perform tasks automatically without human intervention, making relying on external wallets with automatic confirmation impossible [18].

Our Proof-of-concept (PoC) aims to solve the challenge of integrating IoT devices with blockchain technology. It empowers IoT devices to autonomously sign transactions to the blockchain using their authenticated private keys. As a result, it eliminates the need for external wallets to sign transactions, ensuring real-time responsiveness and avoiding potential delays. This approach demonstrates its practicality and advantages, especially in scenarios requiring continuous, automated blockchain interaction through IoT devices. We seek to unlock new possibilities for a more efficient, scalable, and responsive digital ecosystem by bridging these technologies.

This paper presents a PoC that examines the combination of IoT devices and blockchain technology. Our PoC concentrates on eliminating the need for external wallets and enabling IoT devices to automatically sign transactions to the blockchain through their authenticated private keys. This innovative method provides scalability, efficiency, and real-time responsiveness benefits. By allowing devices to handle transaction processing, scalability is improved, enabling more transactions to be processed. Automating transaction signing streamlines the process and lowers overhead, enhancing efficiency. Furthermore, real-time responsiveness is guaranteed, eliminating any delays external wallets may cause. Our research aims to showcase the feasibility and advantages of this method in situations where continuous, automated interaction with the blockchain is required through IoT devices.

The paper is organized as follows: a comprehensive literature review (Section II), overview of blockchain technology and related information to the architecture (Section III and IV), blockchain implementation using the presented methodology (Section V and VII) and, case study and application development (Section VI), and simulation demonstrating the effectiveness of this method (Section VIII), followed by discussion (Section IX). Finally, Section X provides concluding remarks for the paper.

II. RELATED WORK

The integration of blockchain and the Internet of Things (IoT) has garnered significant attention due to its advantages in terms of resiliency and security [19]. Businesses utilizing a unified server-based network structure for transaction acquisition and delivery benefit from this integration, particularly those with moderate transaction volumes. However, the lack of privacy compromises ledger consistency and safety, especially when tracking users' internet activity. To address this issue, many firms are employing blockchain technology to prevent interference and forgeries, developing strategies and procedures that ensure immutable record security for storage and peer-to-peer network communication within and outside the network [32].

To ensure security and transaction efficiency, Huang et al. [33] propose a consensus technique for connected components that reduces legitimate energy expenditure while increasing processing difficulty for malicious actors. The benefits of integrating blockchain and IoT can be summarized in seven aspects: decentralization, scalability, identity, autonomy, reliability, security, and the services market. One area where the lack of transparency is exposed is the agriculture supply chain, which is susceptible to consistent fraud [34]. Several studies have explored the potential uses of blockchain technology in various fields, focusing on its application in IoT systems and associated properties such as privacy, scalability, and record governance [35].

There is a consensus that blockchain technology can enhance visibility throughout the supply chain for agricultural commodities. Businesses are leveraging blockchain and IoT to provide consumers with safe, sustainable, and progressive food production methods. The combination of blockchains, data science, and sensor technologies has led to new ideas for improving resilience in agricultural food supply chains [36]. To address the challenges in conventional agro supply chain networks, Bhat et al. [37] propose the Agri-SCM-BIoT architecture, which also categorizes security risks associated with IoT infrastructure and reviews current blockchain-based defenses.

Minoli et al. [38] discuss various safeguards for blockchains, highlighting the ability of networked devices to gather information, process it, and make sound suggestions. The goal of IoT is to equip a large number of items with digital intelligence for tracking and regulation using algorithms and computational tools [39]. However, challenges related to storage capacity, security, data privacy, and smart contracts have been identified in the blockchain-IoT connection, particularly food traceability.

A ledger solution for energy-efficient IoT streaming devices is proposed to address these challenges, enabling data transfer in independently verified, encrypted, and trustworthy chunks without compromising security, traceability, or trustworthiness [40]. The solution incorporates a proxy re-encryption network to safeguard the data IoT devices transmit. IoT utilizes the Interplanetary File System (IPFS) for file storage and exchange to handle the constant data stream. A security analysis is also conducted on smart contract code to ensure its resilience against vulnerabilities [41].

In transportation, the blockchain and IoT in storage containers promise to improve efficiency and reliability. By utilizing smart contracts and Internet-connected containers, the prototype aims to examine the long-term viability of this technology in transportation.

The architecture proposed by Bahga and Madisetti [42] focuses on the Industrial IoT (IIoT), where blockchain enables sensors to connect and interact with each other. This architecture allows for data storage, analysis, and execution of smart contracts on cloud-enabled single-board computers. The authors demonstrate the potential applications of this platform in machine upkeep and intelligent monitoring.

Angrish et al. [43] propose a decentralized platform called FabRec for sharing information about product construction in a trustworthy network. By using blockchain and smart contracts, this platform enables transparency and direct inspection of manufacturing capabilities. It provides a reliable way for companies to collaborate and share data in the context of mass customization.

Papadodimas et al. [44] present a market infrastructure for trading weather sensor data over the Ethereum blockchain. This infrastructure utilizes smart contracts to record details of each weather sensor and enables the data owner to decide where it will be stored. Using tokens, IoT data can be bought and sold securely and transparently.

Bora et al. [45] present a system, TPPSUPPLY, for supply chain traceability that uses smart contracts to protect users' privacy from intruders. In TPPSUPPLY, off-chain and on-chain smart contract integration uses ECDSA protocol cryptographic methods to enable digital signature and verification. The system can be readily incorporated into any industry, from the food and drug supply to many other application areas that protect privacy.

Hasan et al. [20] suggest integrating blockchain and IoT to improve the agricultural supply chain in Bangladesh. The research recommends using Hyperledger Sawtooth API for product tracking and mobile banking for digital payments. This model aims to increase transparency, prevent delays, reduce errors, and prevent unethical actions. The study introduces an Integrated Agri-Food Supply Chain (IASC) Model to benefit all stakeholders, especially small-scale farmers, and consumers, while providing a roadmap for further research. Oudani et al. [21] propose a green blockchain framework for safely transporting hazardous materials. It includes two models for efficient energy management during transactions, optimizing computing tasks, and reducing CO2 emissions. The prototype shows feasibility in a simulated IoT-based supply chain, promoting sustainable blockchain transactions while ensuring secure transportation of dangerous goods. Chandan et al. [22] suggested that blockchain, AI, and IoT can combined to create a sustainable information

TABLE 1. Comparison table of literature reviews.

Reference	Area	Smart Contract	Platform	Solution Approach
Wenhua et al. [14]	Intelligent manufacturing, finance, the Internet of things (IoT), medicine and health	No	NA	Literature review
Zhu et al. [15]	Data Management	Yes	Ethereum	Prototype
Turkanovic et al. [16]	Global higher education credit platform-EduCTX	No	Ark	Prototype
Dagher et al. [17]	Electronic health records	Yes	Ethereum	Framework
Bhushan et al. [18]	Blockchain based IoT (BIoT) applications	Yes	NA	Proposed model
Chen et al. [19]	Medical / Pharmaceutical	Yes	NA	Literature review
Hasan et al. [20]	Agri-Food Supply Chain	No	Ethereum	Literature review
Oudani et al. [21]	Energy management	Yes	Ethereum	Architecture and mathematical model
Chandan et al. [22]	Food supply chains	No	NA	Analysis
Nanda et al. [23]	Medical supply chain	Yes	Ethereum	Prototype
Popli et al. [24]	Narrowband internet of things	No	NA	Literature review
Chettri and Bera [25]	5G wireless systems	No	NA	Literature review
Kushwaha et al. [26]	NA	No	NA	Literature review
Seven et al. [27]	Virtual Power Plant	Yes	Ethereum	Prototype
Al-Rakhami and Al-Mashari [28]	Supply chain system	Yes	NA	NA
Khan et al. [29]	Short-range communication technologies, radio frequency identification (RFID), middleware, and cloud computing	No	NA	Application
Viriyasitavat et al. [30]	Smart devices and cyber-physical systems	Yes	NA	Architecture
Babaei et al. [31]	Three-level supply chain network	No	NA	Model

system. However, their implementation and integration can be challenging for SMEs, requiring expert knowledge. Effective training platforms are essential for non-specialists to use these technologies. Nanda et al. [23] proposed a new approach called NAIBHSC that combines Blockchain with IoT to create a smart health supply chain management system that ensures security, privacy, trust, and tracking of medical products. It prevents counterfeit drugs and damage to medical components, reduces costs, and offers real-time status updates during shipment. The experimental results showed that it outperformed existing approaches regarding response time, with an average TPS of 100 milliseconds for a group of 500 users.

Overall, these studies demonstrate the potential of blockchain technology in enhancing various aspects of IoT applications. They address challenges such as transaction processing, data sharing, transparency, and collaboration, paving the way for widespread implementation of blockchain in IoT domains. IoT research studies mostly focus on sensors responsible for gathering information. However, our proposed Proof of Concept (PoC) takes a step further by actively writing data directly to the blockchain. This signifies a device that collects information and performs actions based on it. Table 1 summarizes and compares the existing work.

III. SYSTEM MODEL

In this section, we provide a comprehensive introduction and definition of the key components that form the foundation of our system model.

A. BLOCKCHAIN TECHNOLOGY

Blockchain, also known as distributed ledger technology, is a decentralized system that stores data across multiple servers worldwide. Its origin can be traced back to Satoshi Nakamoto's whitepaper on Bitcoin in 2008 [46], which introduced the concept of using blockchain in financial applications. Initially, blockchain technology was predominantly utilized in the financial sector to create a trustworthy and secure environment without a central authority. It addressed issues such as preventing double-spending attacks, where digital assets like cryptocurrencies played a significant role [47]. Over time, the potential of blockchain technology has extended beyond finance and has found applications in various sectors such as supply chain management, healthcare, and more [48], [49]. A blockchain consists of chronologically linked blocks containing cryptographically linked data to the previous block, forming an immutable chain. Any attempt to modify data in a previous block would result in changes to subsequent blocks, allowing the detection and rectification of

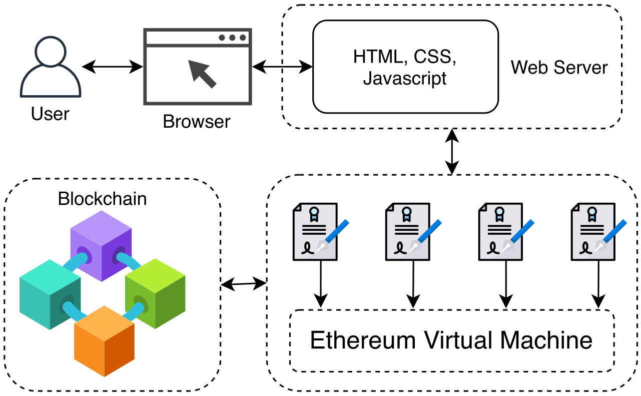


FIGURE 1. Decentalised application (DApp)'s architecture.

tampering [50], [51]. This property ensures the security and immutability of the blockchain.

Cryptocurrencies have a safeguard that prevents attackers from taking control of a blockchain network. This is because they would need to acquire at least 51% of the network's computing power, which is practically impossible [52]. This protection ensures that other miners can continue creating new blocks without disruption. Blockchain-based applications are highly secure, trustworthy, cost-effective, and transparent [53], [54], [55]. Therefore, blockchain technology is a promising solution for many scenarios.

1) ETHEREUM AND DECENTRALIZED APPLICATION

Following the emergence of Bitcoin, numerous alternative cryptocurrencies, commonly referred to as altcoins, have emerged. Ethereum has gained significant popularity as the second most prominent cryptocurrency. Ethereum has introduced a unique platform that enables the development of blockchain projects on top of its blockchain infrastructure [56]. As an open-source, decentralized software platform, Ethereum revolutionized the blockchain landscape by introducing the concept of smart contracts and decentralized applications (DApps) in 2015 [57].

By leveraging the Ethereum Virtual Machine (EVM), developers can build and deploy DApps, digital applications that operate on the blockchain, or a peer-to-peer network of computers without needing a central authority [27]. Smart contracts, a fundamental aspect of Ethereum, define the terms, conditions, and functionalities that govern the execution of agreements on the blockchain [26]. For instance, a smart contract can facilitate a payment transaction between two individuals by programmatically enforcing predefined conditions. This eliminates intermediaries and enables secure and transparent transactions within the Ethereum ecosystem [58]. The DApp (Fig. 1) is connected to a blockchain network, which enables users to perform actions based on the smart contract. Users interact through a front-end interface to transactions of a smart contract to communicate with the blockchain to process and record these actions securely and transparently. Users who interact with a DApp to perform activites follow the same actions.

Essentially, Ethereum functions as a vast global network of interconnected nodes, each maintaining a copy of the Ethereum blockchain [59]. These individual computers form a decentralized infrastructure, providing a robust and distributed computing environment. Transactions within the Ethereum network are disseminated through replicated nodes, ensuring information propagation [60]. This decentralized architecture underpins the security and resilience of the Ethereum blockchain, enabling participants to engage in trustless interactions and transactions worldwide [61].

B. INTERNET OF THINGS

The Internet of Things (IoT) is a highly advanced network of physical objects with the remarkable ability to communicate and connect seamlessly over the Internet [62]. These objects are designed to expertly gather valuable data from their surroundings, ultimately leading to more efficient processes, cost savings, and improved product quality. The physical devices are at the core of an IoT system, often equipped with sensors and actuators [63]. These devices range from everyday objects like thermostats, lights, and appliances to more advanced devices like industrial machinery and vehicles. Each device is assigned a unique identifier and is connected to the internet through wireless or wired connections [64].

The advanced microprocessors integrated into the IoT devices make them fully equipped to connect, gather data, and make smart decisions autonomously, resulting in unprecedented productivity and convenience [29]. Sensors embedded within the devices capture information to perform specific actions based on received instructions. The use of blockchain technology for digital currency transactions has become common. Recent developments in sensor technology (Internet of Things) have also shown indications of optimism [28]. People who might not otherwise be able to exchange content can do so through blockchain technology. Without IoT optimization of the distributed ledger, businesses risk significant inefficiencies and the need for significant processing capacity.

C. MICROPROCESSOR

IoT systems depend on microprocessors, crucial in executing numerous tasks [65]. These tasks encompass data acquisition, actuator activation, device-to-device communication, operating system (OS) management, program execution, power management, and beyond. The Raspberry Pi is a favoured choice among the available microprocessors for consumer applications [66]. Its compact size and cost-effectiveness make it highly suitable for development purposes. It features an ARM architecture that allows users to build applications on established operating systems like Linux [67]. In enterprise usage, notable microprocessor manufacturers such as Intel, AMD, and Qualcomm offer prominent solutions. It is vital to recognize that without these fundamental components, the IoT industry as we know it would not be feasible, as they form the backbone of IoT device functionality and enable the realization of its vast potential [25].

D. MICROCONTROLLERS

Microcontrollers are pivotal in the Internet of Things (IoT) by providing control and monitoring capabilities for various devices and systems. These devices offer cost-effective, compact, and energy-efficient solutions, making them well-suited for performing specific tasks across various gadgets [24]. A standard microcontroller encompasses components such as the processor, memory, serial ports, and peripherals, including timers and counters. In our research, we have selected the Arduino Uno microcontroller as our preferred choice for prototyping purposes. The Arduino Uno stands out due to its seamless communication capabilities via a virtual serial port with computer systems [68]. This enables effortless control and coordination of various input-output devices, enhancing the overall efficiency and functionality of IoT applications.

1) INPUT DEVICES

A connection is established between the Arduino Uno and different input devices to obtain information. These devices serve as crucial tools for gathering data and can be classified into the following categories:

1) ***Sensors:***
   - ***Temperature and humidity:*** Sensors, such as DHT11 or DHT22, enable the monitoring of ambient temperature and humidity levels.
   - ***Motion:*** Passive Infrared (PIR) or ultrasonic sensors detect motion or presence, enabling applications such as security systems or occupancy detection.
2) ***Buttons and Switches:***
   - ***Push Buttons:*** Simple momentary pushbuttons provide user input for various applications, including user interfaces or menu navigation.
   - ***Toggle switches:*** These switches have two stable states and are commonly used to control system functionalities or modes.
3) ***Potentiometers:*** Variable resistors enable users to input analogsignals by manipulating a physical knob or dial. By precisely adjusting the position of the knob, users can finely tune and modulate the desired output or response, enhancing the flexibility and customization of various electronic systems.

2) OUTPUT DEVICES

While the data is being retrieved, the Arduino Uno can be connected to various output devices to display the information or perform programmed actions based on the input received. Below are some output devices that are compatible with the Arduino Uno:

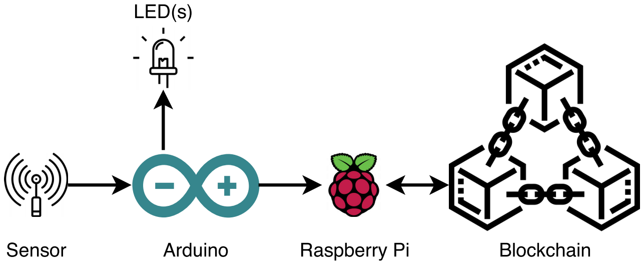


FIGURE 2. IoT integration with Raspberry Pi for blockchain communication.

1) ***LEDs (Light-Emitting Diodes):*** are great for visual or status indications in applications. RGB LEDs offer even more possibilities by displaying a wide range of colours, making them perfect for visually engaging displays and colour-coded visual cues in IoT systems.
2) ***Buzzers:*** are sound-producing devices that can generate basic audio tones or be used for audible alerts and notifications.

IV. IoT SYSTEM DESIGN

Fig. 2 shows the full IoT device communicating with the blockchain network. We interface Arduino with Raspberry Pi such that the sensor's value from Arduino sends values to Raspberry Pi through a simple serial communication [69]. As per our use case, we use one-way communication, i.e., the information is sent from Arduino to Raspberry Pi. The Raspberry Pi's GPIO pins are digital pins that set outputs or read inputs to high or low. To read the value of the analog input devices such as potentiometers, one might use an ADC chip (Analogue-to-Digital converter) like $MCP3008$ [70].

In our system design, we used Arduino instead of IC $MCP3008$ because, for the proof of concept, we used Arduino for the analog inputbecause it fullfilled the same criteria of our requirement, i.e., getting analog input from the sensor.

The Adruino (setup described in section IV-A) one-way communicates by sending values to raspberry pi, which interacts with the blockchain in writing and reading information directly (detailed description in section V-A).

A. ARDUINO SETUP

Fig. 3 shows Arduino's circuit architecture. We used Arduino Uno R3 because it is popular, has good documentation to get started, and is quite easy to use. The circuit consists of the following:

- **Arduino Uno** to load the program that will take input from the 10 kΩ potentiometers and, based on input range, will give output signal through different LEDs.
- **LEDs** of different colors indicate the analoginput range from the potentiometer. The LED that should illuminate is coded and loaded. The algorithm 1 describes the output range.
- **10 kΩ potentiometer** is used as input. It is a three-terminal adjustable variable resistor to alter the resistance via a knob or dial. The potentiometer's

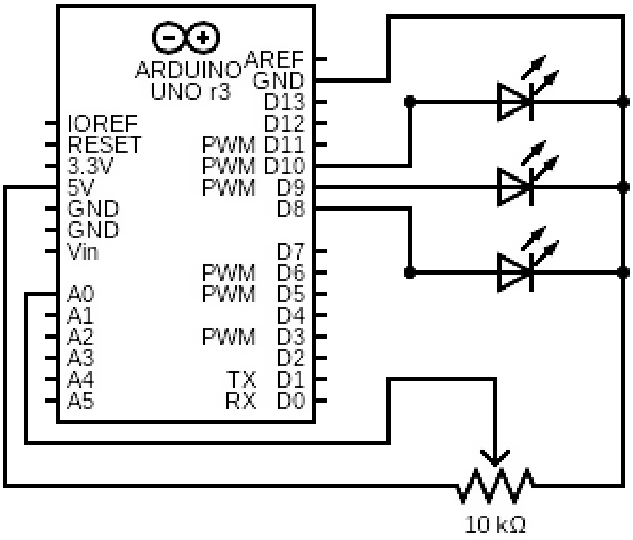


FIGURE 3. Arduino schema.

rotation changes the amount of resistance, giving a different analoginput. The shaft's rotation varies from 0 to $5V$, giving an analogread from 0 to 1023. This range is proportional to the voltage applied to the pin.
We use the potentiometer as input to demonstrate how by manually simulating the input (using the knob), we can alter the input value to make a desired environment. For example, using a humidity sensor or temperature might not have been a good choice because controlling the environment as per our input would have required an external environmental setup, making the experiment comparatively expensive and difficult to control.

- **Jump wires** of different types are used for communication among different entities.

B. RASPBERRY PI SETUP

Our prototype utilizes the **Raspberry Pi 3 Model B+**, a low-cost computer that is about the size of a credit card. It can be connected to input devices such as a keyboard and mouse and can be displayed on external devices like monitors or televisions. The device is powered by a `BCM2837B0` System-on-Chip (SoC) that includes a 1.4 GHz quad-core `ARMv8-A` 64-bit processor.

1) ACCESS OVER SSH

To get started, we must ensure that our device is connected to the local network and to wifi on our Raspberry Pi. We will need the device's local address to proceed. For added security, SSH is disabled by default to prevent unauthorized access from hackers. A private key is stored in the device to ensure maximum protection. To access the device, we will need to enter a password added is set up on the Raspberry Pi. It's recommended that we change the default password for added security.

Algorithm 1 Arduino Setup

```
GREEN ← 10
YELLOW ← 9
RED ← 8
ANALOG_IP ← A0
function SETUP()
    pinMode GREEN ← Output
    pinMode YELLOW ← Output
    pinMode RED ← Output
end function
loop
    value ← analogRead(ANALOG_IP)
    if $value \le 600$ then
        digitalWrite GREEN ← HIGH
    end if
    if 601ł$value \le 800$ then
        digitalWrite YELLOW ← HIGH
    else
        digitalWrite RED ← HIGH
    end if
     Print value
end loop
```

We connect to the device via a remote desktop for a seamless and easy experience.

2) DEVICE REGISTRATION

The administrator manages the Internet of Things (IoT) devices within a supply chain scenario. The administrator registers the IoT device on the smart contract, associating it with a specific product ID. This registration formally acknowledges that the IoT device is authorized to participate in the supply chain operations. The IoT device is physically installed on a transport vehicle, allowing it to engage with the blockchain network actively. The IoT device maintains a continuous connection with the blockchain throughout transportation, enabling it to commit transactions to the distributed ledger. These transactions typically pertain to various stages of the product's journey, such as location updates, temperature monitoring, or other relevant data points.

The IoT device is authenticated with a private key and the corresponding address associated with its registration on the smart contract. This authentication mechanism guarantees that only the authorized IoT device can interact with the blockchain network and commit transactions on behalf of its associated product.

Once the product associated with the IoT device reaches its intended recipient, the device is reset, marking the completion of the product delivery. It signifies that the IoT device's role in the supply chain for that specific product has concluded. The reset process may also involve deregistering the IoT device from the smart contract. This step prevents any unauthorized use or tampering with the IoT device once its purpose in

Algorithm 2 IoT Contract Communication

```
Required: Smart Contract Address, ABI
Required: Blockchain API URL
Required: Dotenv with privatekey
Required: timeGap $\leftarrow$ From Smart Contract
Import required libraries
 Establish Connection with Network
productID $\leftarrow$ ID of Product
iotc $\leftarrow$ contractInstance(Address,ABI)
function inject_Transaction(value)
    Broadcast transaction passing productID and value
end function
Import PrivateKey
 Connect to Arduino Port
starting_time $\leftarrow$ currentTime
tranaction_value $\leftarrow$ 0
while True do
    sensorValue $\leftarrow$ Read Sensor Value
    if sensorValue $> 0$ then
        sensorValue $\leftarrow$ Value from Arduino
        if sensorValue > tx_value then
            tx_value $\leftarrow$ sensorValue
        end if
        if currentTime $\geq$ starting_time + timeGap then
             INJECT_TRANSACTION(tx_value)
            starting_time $\leftarrow$ currentTime
            tx_value $\leftarrow$ 0
        end if
    end if
end while
```

the supply chain is fulfilled. If required, the device can be reauthenticated with new key pairs for a new product .

This device is a connected vehicle communicating with a smart contract within a designated timeframe. Users can view information from the device through a user interface. Figure 4 outlines the steps for a product with a specific identification number or serial number, including Initialization, where the product is initialized with important information such as its source and destination. In the Transfer phase, the device updates the data at regular intervals of approximately 20 seconds. Once the product is received, the device stops updating the blockchain with information. Figure 4 shows the device's integration with a transport vehicle. In this example, the IoT device monitors the temperature of a refrigerator. The IoT device communicates with the blockchain remotely.

C. SECURITY

The device is connected to the local network for configuration to a secure Wi-Fi network, ensuring that the device can access the internet and communicate with other devices within the network. The device is protected from unauthorized access through a secure connection, and various measures are implemented in Raspberry Pi's setup. Additionally, SSH is enabled by default to prevent hackers from gaining access to the device and its private key, which contains sensitive information. Additionally, the Rasppi is password protected and requires a separate login using the password associated with the Raspberry Pi. Adding an extra security layer ensures that only authorized individuals can access the device and its resources. While a default password is initially set, changing the password to a unique and strong one is strongly recommended to enhance security further.

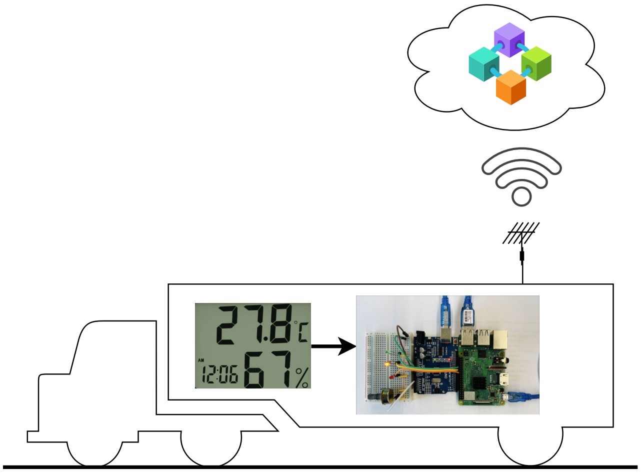


FIGURE 4. IoT device fitted to transport communicating with the blockchain.

1) SMART CONTRACT ACCESS INFORMATION

The smart contract incorporates a verification mechanism to determine whether the required time for executing the contract has elapsed. The transaction will be rejected and not broadcasted if the designated time passes. However, the smart contract will broadcast the transaction for further processing if the required time has elapsed. This time-based validation ensures that transactions are executed per the specified timeframe specified in the contract, promoting transparency and adherence to temporal constraints.

In addition to the time checks the smart contract performs, we introduce an additional layer involving a Raspberry Pi. The Raspberry Pi is programmed to verify the required time in the smart contract before broadcasting at its level. It ensures that the necessary time has elapsed before proceeding with the broadcast.

2) SSH FOR PUBLIC KEY AUTHENTICATION

To improve the convenience and security of storing and accessing private keys, using the dotenv library is recommended. This library allows the creation of a separate '.env' file. This approach centralizes the storage of private keys in a secure and easily accessible location, making it easier to manage and deploy scientific applications. The '.env' file stores private keys in key-value pairs, ensuring confidentiality. With the help of dotenv, accessing private keys becomes more straightforward and secure [71].

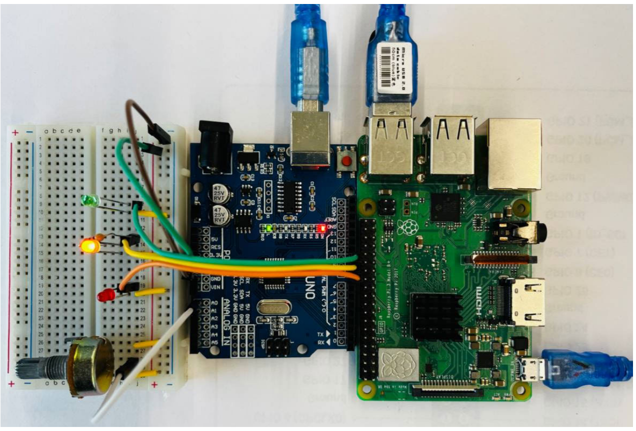


FIGURE 5. IoT device consisting of Potentio meter, LED lights, microcontroller Arduino UNO, and microprocessor Raspberry Pi.

V. METHODOLOGY

Our approach involves creating an architecture that combines IoT and Blockchain technology. This architecture will be used to develop and test an IoT layer that collects sensor data and communicates with the blockchain network. To collect data, we will use an IoT device (See Figure 5) that interacts with the application deployed on the private blockchain network. The microcontroller reads information and executes virtual scripts based on the input, which is later injected into the blockchain. The device periodically sends updates to the blockchain with the sensor's value. However, continuous communication over the blockchain can be expensive, therefore the device will update the blockchain value at a specified interval determined by the smart contract. We thoroughly tested the system to ensure its functionality, security, and reliability. Any bugs or issues identified during the testing were addressed, and necessary refinements were made (section VII-E).

A. DEVICE TRANSACTION SIGNATURE

Every transaction added to the blockchain will be approved by an IoT device, i.e., without using decentraliszd external wallets such as MetaMask.

External wallets like Metamask and Wallet Connect allow users to interact with DApps and smart contracts on blockchains. These wallets are integrated into EVM-based applications like Ethereum, Binance, Arbitrum, Polygon, etc. They enable users to access their EVM accounts and interact with smart contracts. Users manually approve transactions signed, for example, by Metamask using their private key to ensure authenticity and integrity. The signed transaction is then broadcasted to the Ethereum network via the Metamask provider, which includes relevant details such as the recipient address, transfer amount, and additional smart contract data. Metamask streamlines the transaction signing and broadcasting process, offering a user-friendly interface for managing Ethereum accounts and engaging with smart contracts and DApps on the Ethereum network [72].

The IoT device is designed to sign transactions without manual intervention automatically periodically. It is programmed to allow it to interact directly with the smart contract and use the authenticated private key for transaction signing (refer section IV-C). Algorithm 2 describes the device's interaction with the smart contract on the blockchain to sign and broadcast the transactions, thus ensuring the integrity and validity of the transactions it initiates. This automated transaction signing capability enhances the efficiency and reliability of the IoT device's involvement in the supply chain or any other relevant application where its autonomous interaction with the smart contract is required.

VI. WORKFLOW

Section IV provided the solution of an IoT-based device integrated with the smart contract.

Workflow of the system:

1) In deploying a smart contract on a blockchain network, a wallet address is associated with the role of the contract owner.
2) The smart contract owner grants access to the item's producer, who must verify access with the smart contract before performing actions. The contract processes or reverts actions based on access verification.
3) The producer, with granted access, creates a product by providing relevant information such as destination, recipient, and the integrating IoT device known as the Transporting Entity. The Transporting Entity continuously communicates over the internet, updating the transport status. The device periodically updates the blockchain with sensor values within a specified interval to minimize costs read from the smart contract.
4) The IoT device interacts with the smart contract, following an algorithm 6 that interfaces with device actions and internal smart contract actions. The device sends sensor values to the contract, storing them and comparing them with previous values at the end of each time frame. The value is broadcastbased on specified criteria (higher or lower) at the end of the time frame. The following are the off-chain steps that IoT device carries out:
    a) Sensor every second notes the value and stores the variable.
    b) Depending on the time frame to broadcast the transaction, every second the value read is compared and with the preceding value, comparing higher or lower (depending on the requirement), is stored in the variable broadcasted at the end of each time frame.
5) The previous step is repeated until the package is received. Once the package is received, the sensors can still read values, but the transaction cannot be committed to the blockchain. (Algorithm 5).

Figure 6 represents the sequence workflow of the proposed IoT model. The transport entity interacts directly with the blockchain whereas other entities interact with blockchain via DApp (explained at III-A1)

VII. BLOCKCHAIN BASED IoT SOLUTION

This section will demonstrate the practical application of IoT-based solutions in a blockchain and their integration with a basic supply chain scenario.

A. USE CASE

Imagine an object needing to be transported from its source to a specific destination while complying with certain requirements to guarantee its optimum effectiveness. If the object is exposed to harsh or unfavorable conditions during transportation, its efficiency may be compromised. However, the individual receiving the object at the destination may not know the transportation conditions and may still accept the object as if it had been transported under favorable conditions. To avoid this issue, Blockchain technology can monitor and report the object's progress from its origin point to its ultimate destination, ensuring its requirements are met throughout the journey.

We define a simple scenario where a producer sends an item to a receiver through a transport company, and here, it is important to emphasize that we are solely focusing on a single transport company for the delivery of an item from a producer to a receiver.

B. ACTORS

The scenario involves the following participants:

1) **Admin**: The administrator must ensure the producer is authorized to create items and a smart contract based on the specific use case. In our proof of concept, the administrator is responsible for the following activities:
    a) **Grant Access**: The administrator can permit specific wallet addresses, assigning them the producer role. This role authorizes them to create a package on the blockchain.
    b) **Revoke Access**: The admin can also revoke producer access.
2) **Producer:** To facilitate the production process, the authorized Producers can utilize the function within the smart contract and input the required parameters. Among these parameters is the designated transporter's wallet address, which will be responsible for physically transferring the item to its intended destination.
3) **Transporter:** The notion of a transporter may vary depending on the situation. In this instance, we allude to a platform where an IoT device is incorporated to gauge particular conditions. To clarify, it could be a moveable refrigeration unit that gauges temperature or a freight vehicle that consistently relays data on its whereabouts.
4) **Receiver:** The receiving entity that will receive the item.

C. BACKEND: SMART CONTRACT DESIGN

Blockchain technology offers a high level of security, and access control is a crucial feature that ensures its integrity. This is achieved through smart contracts, which enable transactions to be signed by the intended recipient. We used the EVM test network Binance and the Hardhat framework to develop and deploy our smart contract [73]. The latter provides several benefits, including Solidity debugging, testing, and comprehensive documentation, which make it easier for new users to learn and use the platform. Deploying our smart contract on the Binance test network was strategic since it offers low fees and fast transaction processing times. Furthermore, using a test network allows us to make enhancements to the blockchain independently of the main network without any capital involvement. Utilizing these resources has allowed us to create a robust and secure system that benefits our users.

1) ACCESS CONTROL

System actors operating within the system are granted the ability to input information by accessing the smart contract. Following the system's architecture, the smart contract owner is held accountable for providing producers with access to create packages or products. It is presumed that the individual who deploys the smart contract is the initial owner, though ownership has the potential to be transferred. Algorithm 3 details the process for granting or revoking access, which the smart contract owner or the system administrator can execute.

Algorithm 3 Granting/Revoking Access

```
Input: address_user
Initialization: $userAccess(address\_user) \leftarrow bool$
function _toggelAccess(_address,_value)
    $userAccess(\_address) \leftarrow \_value$
end function
if ($msg.sender = address\_owner$) then
    currentState $\leftarrow$ userAccess(address_user)
    if ($grantAccess$) then
        if ($currentState \neq True$) then
            _toggelAccess(address_user,True)
        else
            Revert: "Already has access"
        end if
    else
        if ($revokeAccess$) then
            if ($currentState \neq False$) then
                _toggelAccess(address_user,True)
            else
                Revert: "No access"
            end if
        end if
    end if
else
    Revert and show error "Only Owner"
end if
```

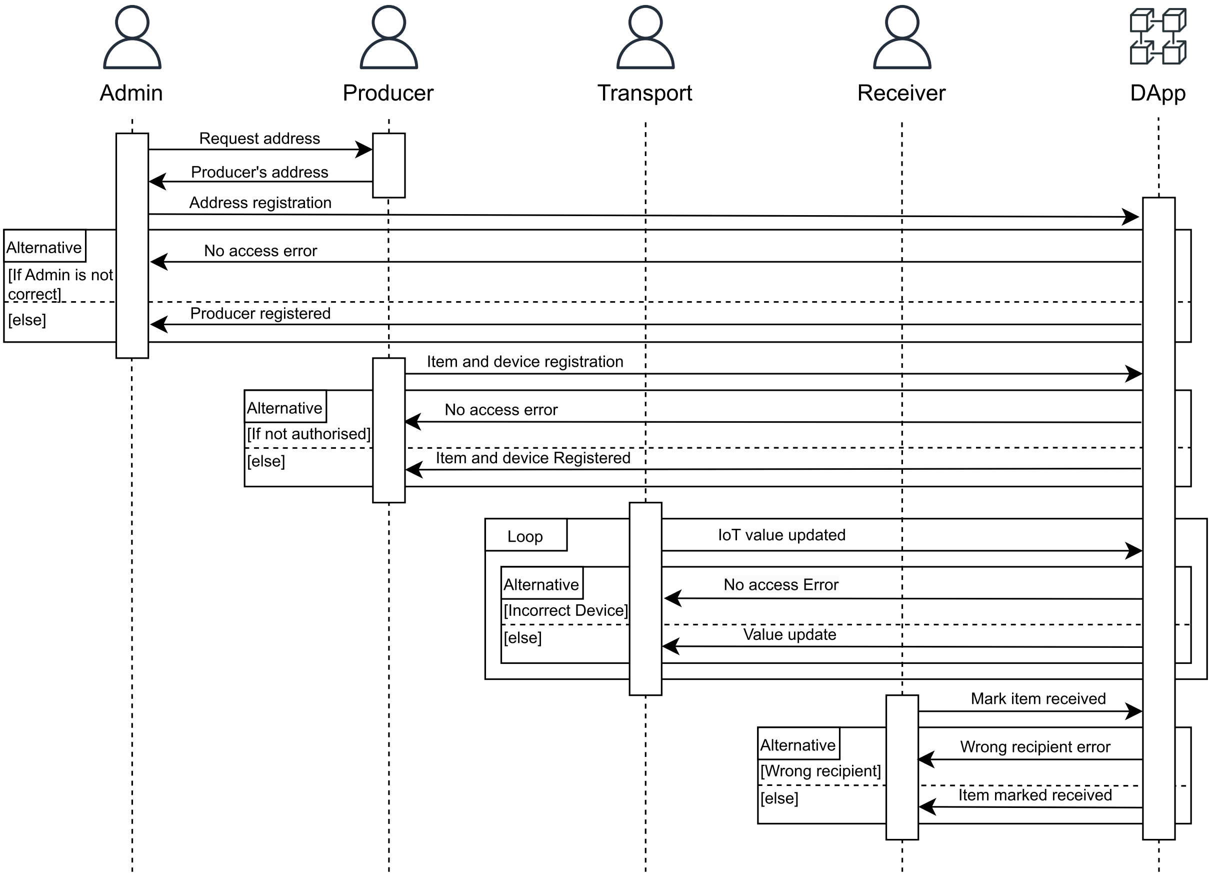


FIGURE 6. **Workflow sequence diagram.**

Algorithm 4 Initializing Product

```
Input: destination, recipient, transport
Initialization: $currentID \leftarrow ID$
if ($userAccess(address\_user) = True$) then
    $map[currentID].destination \leftarrow destination$
    $map[currentID].recipient \leftarrow recipient$
    $map[currentID].transport \leftarrow transport$
    $ID++$
else
    Revert and show error "Only Producer"
end if
```

2) INITIALIZE PRODUCT

Once a producer receives access to the system, they can start initializing (producing) package items.. We consider product serial numbers in incrementation (starting from 0) for simplicity. The function *Initialize Product* passes the following parameters:

- *destination:* Destination of the item from origin.
- *recipient:* The recipient's address, i.e., the package receiver.
- *transport:* Here, we mean the IoT device integrated into a vehicle. The vehicle is communicating with the blockchain via the IoT device.

3) RECEIVE PRODUCT

After the product reaches its destination, the smart contract returns the recipient's address of the product with passed *productID* as the parameter. The algorithm 5 verifies that the receiver is correct as intended. The product's received status is marked *true* if verified.

Algorithm 5 Receive Product

```
Input: productID
if ($Product\_recipient \neq msg.sender$) then
    if (Product not received) then
        $map[productID].received \leftarrow True$
    else
        Revert with error: "Product received"
    end if
else
    Revert with error: "Only Recipient"
end if
```

4) TRACK PRODUCT

The IoT device communicates with a blockchain network to update sensor values or conditions at specific intervals defined in a smart contract algorithm 6. The IoT device has a package serial number that enables it to accurately assign values to specific products . The smart contract verifies that the signer is the authorized entity for the required package.

A time constraint is enforced to ensure the integrity of the data and prevent consecutive transactions from being committed prematurely. If the required time has not elapsed since the previous transaction, an error is thrown, thereby necessitating the implementation of a layer-2 solution. This layer-2 solution safeguards, preventing the device from broadcasting a transaction before it is deemed permissible (Described at IV-B). To address this requirement, Algorithm 2 has been devised as the proposed solution, effectively ensuring that such untimely transactions are prevented and maintaining the reliability and accuracy of the data recorded on the blockchain.

Algorithm 6 Track Product

```
Input: productID, value
Input: timeGap from contract
if ($Product\_recipient \neq msg.sender$) then
    if (Product not received) then
        $currentTime \leftarrow block.timestamp$
        $previousTime \leftarrow previousTime(productID)$
        if currentTime $\geq$ previousTime then
            $previousTime(value) \leftarrow value$
            $previousTime(productID) \leftarrow currentTime$
        else
            Revert with error: “Required time not passed”
        end if
    else
        Revert with error: “Product received”
    end if
else
    Revert with error: “Only Transport”
end if
```

D. FRONTEND: USER INTERFACE APPLICATION

Blockchain networks offer blockchain explorers [74] as interfaces to interact with deployed and verified smart contracts. The usability of these explorers can be challenging. This is because they provide standardized solutions across the network for all smart contracts, which may align differently with the specific needs of each application. Therefore, developing a user interface can significantly enhance the application workflow and improve the overall user experience. Customizing the interface to fit the application's needs can enhance user experience. It enables them to interact more smoothly and efficiently with the smart contracts.

We created a decentralized application with various components allowing different users to interact. Frontend development is crucial in displaying data and enabling user interactions. We utilized the Vue framework [75], a JavaScript framework known for efficiently constructing dynamic and interactive web interfaces, to achieve this. Vue's reactivity and component-based architecture make development more straightforward. Additionally, we integrated Tailwind CSS, a utility-first CSS framework, to further enhance the application's frontend design.

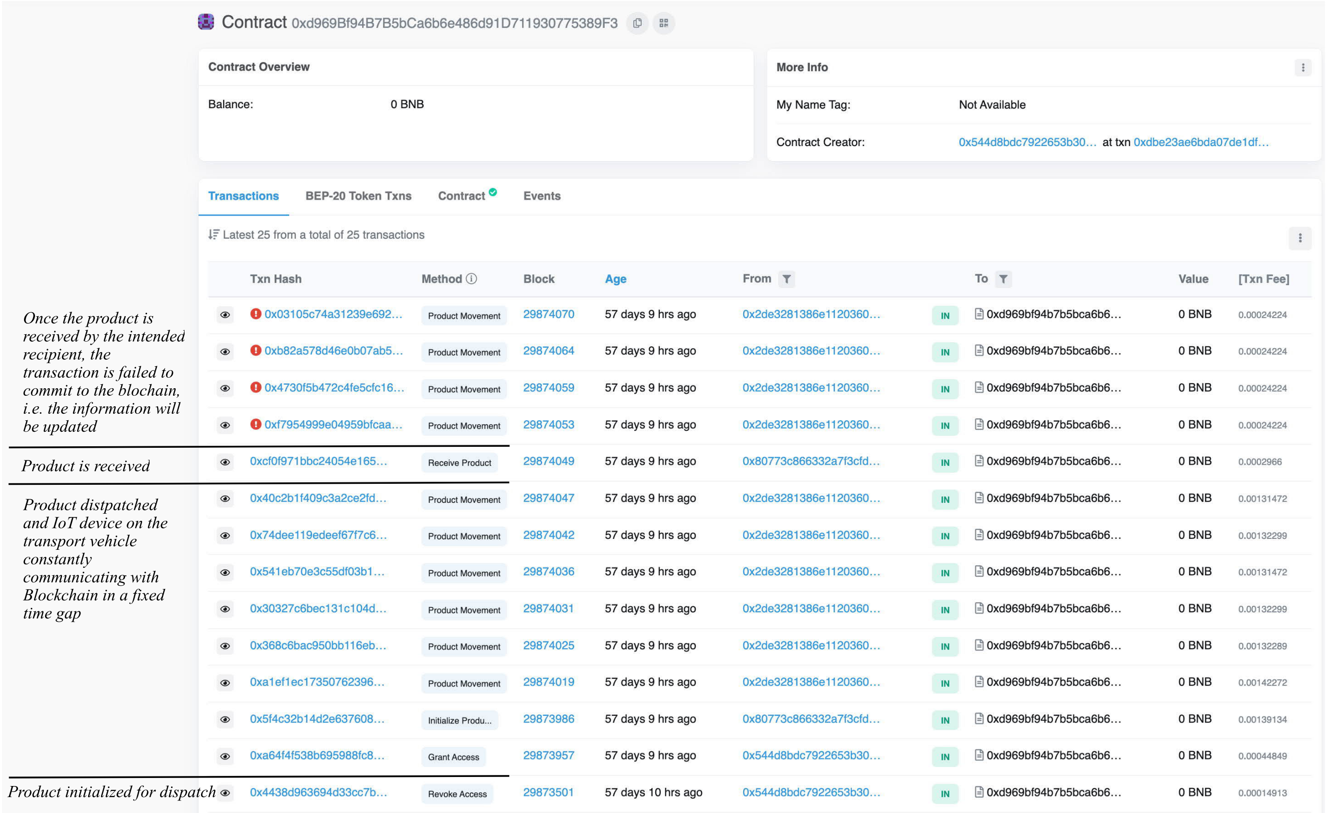
In decentralized applications (DApps) and blockchains, communication often occurs through Remote Procedure Calls (RPC) [76]. RPC enables DApps to interact with the blockchain by calling smart contract functions, obtaining data, and carrying out transactions. This approach allows DApps to benefit from the blockchain's security and transparency while maintaining compatibility and scalability with external systems and real-time data sources.

The application consists of the following pages:

1) **Admin Page:** is where the Admin can grant or revoke a producer's access to produce packages/items. The Admin can also check the producer's status to see if they have access to the network. Depending on the blockchain's response to the status of the producer's wallet, the Admin will be shown the next possible action. For instance, if the wallet does not have access, the Admin can grant access and vice versa (Algorithm 3).
2) **Producer Page:** Authorized producers can create items by providing the required parameters, such as destination, receiver, and transportation, as outlined in the example workflow. Once all the necessary steps are completed, the producer will receive a package serial number (or tracking number) from the blockchain. The transaction will be committed to the blockchain before the serial number is returned. An error message will be displayed if the wallet address is not authorized to create packages (Algorithm 4).
3) **Receiver Page:** After the authorized receiver receives the packages, they must enter the package serial number to confirm receipt of the product. The algorithm 5 describes the specific actions the receiver should take. An error message will be displayed if the wallet address is not authorized to receive the package.
4) **Track:** To keep track of a package's condition, one must have its serial number and can check its status at specific intervals. The package's sensors provide information on its condition (Algorithm 6).

The application requires a connection to an external wallet to perform any write actions. While it is possible to sign transactions on the smart contract using a private key similar to the proposed IoT device, we integrate using an external wallet for integration with decentralized applications.

Figure 7 demonstrates how a blockchain smart contract interacts with an IoT device. However, if the intended recipient has already received the product, the following transaction, emitted from an IoT device, cannot be committed to the blockchain. A status check can be implemented before broadcasting the transaction to avoid incurring gas fees. Verifying the status beforehand can prevent failed transactions from being executed and associated gas fees. This proactive approach optimizes transaction efficiency and reduces costs in the blockchain network.



Contract 0xd969Bf94B7B5bCa6b6e486d91D711930775389F3

Contract Overview	
Balance:	0 BNB

More Info	
My Name Tag:	Not Available
Contract Creator:	0x544d8bdc7922653b30… at txn 0xdbe23ae6bda07de1df…

Latest 25 from a total of 25 transactions

	Txn Hash	Method	Block	Age	From		To	Value	[Txn Fee]
👁	! 0x03105c74a31239e692…	Product Movement	29874070	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00024224
👁	! 0xb82a578d46e0b07ab5…	Product Movement	29874064	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00024224
👁	! 0x4730f5b472c4fe5cfc16…	Product Movement	29874059	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00024224
👁	! 0xf7954999e04959bfcaa…	Product Movement	29874053	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00024224
👁	0xcf0f971bbc24054e165…	Receive Product	29874049	57 days 9 hrs ago	0x80773c866332a7f3cfd…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.0002966
👁	0x40c2b1f409c3a2ce2fd…	Product Movement	29874047	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00131472
👁	0x74dee119edeef67f7c6…	Product Movement	29874042	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00132299
👁	0x541eb70e3c55df03b1…	Product Movement	29874036	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00131472
👁	0x30327c6bec131c104d…	Product Movement	29874031	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00132299
👁	0x368c6bac950bb116eb…	Product Movement	29874025	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00132289
👁	0xa1ef1ec17350762396…	Product Movement	29874019	57 days 9 hrs ago	0x2de3281386e1120360…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00142272
👁	0x5f4c32b14d2e637608…	Initialize Produ…	29873986	57 days 9 hrs ago	0x80773c866332a7f3cfd…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00139134
👁	0xa64f4f538b695988fc8…	Grant Access	29873957	57 days 9 hrs ago	0x544d8bdc7922653b30…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00044849
👁	0x4438d963694d33cc7b…	Revoke Access	29873501	57 days 10 hrs ago	0x544d8bdc7922653b30…	IN	0xd969bf94b7b5bca6b6…	0 BNB	0.00014913

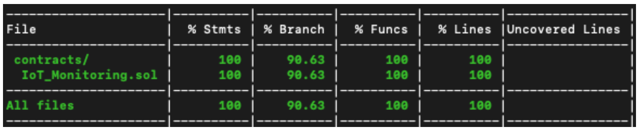
Once the product is received by the intended recipient, the transaction is failed to commit to the blochain, i.e. the information will be updated

Product is received

Product distpatched and IoT device on the transport vehicle constantly communicating with Blockchain in a fixed time gap

Product initialized for dispatch

FIGURE 7. Actions of IoT device's interaction with the blockchain's smart contract. (From bottom to up) Product Initialise, Product transportation phase, Product is received, and transactions not broadcasted once the product is marked received.



```
---------------------|----------|----------|----------|----------|----------------|
File                 |  % Stmts | % Branch |  % Funcs |  % Lines |Uncovered Lines |
---------------------|----------|----------|----------|----------|----------------|
 contracts/          |      100 |    90.63 |      100 |      100 |                |
  IoT_Monitoring.sol |      100 |    90.63 |      100 |      100 |                |
---------------------|----------|----------|----------|----------|----------------|
All files            |      100 |    90.63 |      100 |      100 |                |
---------------------|----------|----------|----------|----------|----------------|
```

FIGURE 8. Solidity code coverage.

E. TESTING SMART CONTRACT

We utilized the Hardhat testing framework to evaluate our smart contract's functionality and security thoroughly. Hardhat provides a robust and efficient testing environment, allowing us to test different scenarios and cases. Through this testing process, we identified and addressed potential vulnerabilities, validated our workflow's integrity, and improved overall quality. Our testing considered numerous real-world conditions to ensure our system could deliver reliable and secure performance in practical deployment scenarios.

We assess the effectiveness of the test by determining how much of the code is executed during test runs. Figure 8 provides the coverage report of the proposed smart contact solution.

The code with instructions is available here [77].

VIII. WORKFLOW SIMULATION

We conducted testing using test cases to evaluate the security of the smart contract (Described in section VII-E). Here, the simulation focuses on assessing the performance of gas consumption.

Measuring gas consumption allows for analyzing and assessing computational resources used by smart contracts. By monitoring gas usage, the effectiveness and efficiency of smart contracts can be improved, leading to increased scalability and cost-effectiveness.

In our simulation, we consider a scenario where a package of cream cheese is transported from New York to California via truck, with multiple stops and drops along the route. The cream cheese requires constant refrigeration to prevent spoilage caused by bacterial growth [78]. To ensure the integrity of the product, the truck is equipped with a specialized refrigeration system that maintains the temperature within the optimal range throughout the journey.

It is essential to have proper ventilation when transporting cheese to ensure that its quality is maintained and spoilage is prevented. This is especially important during longer trips, especially in tropical regions with cold storage facilities. To maintain the flavor and texture of cheese, it should be loaded in new and aged conditions. However, it is crucial to control ventilation carefully to avoid mold growth. While sufficient airflow is necessary, excessive drafts should be avoided as they can cause damage. Balancing

TABLE 2. Gas used in setting the environment.

Action	Executer	Gas Used
Contract Deploy	Owner	2 048 898
Set Conditions	Owner/Admin	68 448
Grant Access	Owner/Admin	46 748
Revoke Access	Owner/Admin	24 825

TABLE 3. Gas used in the workflow. Tracking transport shows the cumulative gas that is used in transportation.

Action	Executer	Gas Used
Produce	Producer	143 482
Track	Transport	1 035 362
Receive	Recpient	29 460

proper ventilation to protect the cheese from unfavorable environmental conditions is a key consideration in achieving successful cheese transportation [79].

A. SYSTEM SETUP

The table 2 displays the amount of gas (measured in Wei) utilized during the system setup to deploy the contract. Additionally, this process defined temperature zones to ensure proper storage conditions. Access rights to authorized wallets, such as Cream Cheese Enterprises, were also granted or revoked.

As of 2023, there are 436 cheese production businesses in the US, which is a 0.9% increase from the previous year. The number of businesses has steadily risen over the past few years, with 408 in 2020, 417 in 2021, 433 in 2022, and 436 in 2023 [80]. We register the 417 address wallet by calling *grantAccess* function and take the average gas used. We infer that one Ethereum block can fit approximately 641 registrations. Despite an overall increase in the number of cheese businesses in the US, for our experiment, we assumed that 50% of these businesses would not continue. As a result, their address wallets must be deregistered through the use of the *revokeAccess* function, and the average gas used must be calculated. It has been inferred that one Ethereum block can accommodate approximately 1208 deregistrations, almost double the previous amount. This is because the *sstore()* opcode is used when updating the wallet mapping to true or false. If the wallet is true, we store 1; if it is false (i.e., 0), we revert to the original state [81].

B. SUPPLY CHAIN WORKFLOW

Once registered, the *Producer* can create products that will be recorded on the blockchain. The package can be produced by inputting the parameters *Destination, Recipient, Transport*. The product is created, returns package ID: 1, and updates the blockchain accordingly. The transportation time to California from New York is approximately six days, assuming the journey takes 43 hours of non-stop driving or 6-7 days with stops. The package's temperature is constantly monitored and updated every 24 hours, indicating the maximum temperature reached. When the package arrives, the recipient receives it. Table 3 summarises the gas used in this process. From the table, we infer that the number of supply chain actions that can fit in 1 Ethereum block is approximately 24 transports, whichmay be independent of the size of the package.

IX. DISCUSSION AND FUTURE WORKS

The smart contract architecture allows the simultaneous management of multiple products without having separate contracts for each product. This design promotes parallelization, allowing multiple products to be processed simultaneously within a single smart contract. The ability to handle multiple products within one contract enhances scalability and efficiency. The concurrent execution of transactions related to different products optimizes resource utilization and improves overall system throughput. This approach eliminates the complexity and potential bottlenecks associated with individual contracts for each product.

When an IoT device has poor signal coverage, it may have trouble communicating and go offline, which makes it unable to connect with the blockchain network. However, this problem has a solution: temporary memory storage can be added to the IoT device. This storage allows the device to monitor its condition and maintain its value. The IoT sensor reads and stores the value in a loop; if the value is higher than the previous one, it replaces it. This ensures that only the highest sensor value is recorded on the blockchain during the offline period, which avoids unnecessary data overload. Timestamps of previous and current transactions can detect when the device is offline and when it is reconnected to the blockchain network. By comparing timestamps, it is possible to determine when the device lost communication and regained connectivity.

Manual data entry can be automated with a scanner like a QR code or barcode reader to simplify product initialization. This approach reduces human error and improves efficiency by automatically capturing relevant data such as product ID, batch number, manufacturing, and expiration dates. This improves traceability and saves time throughout the supply chain [82].

There is a risk of fake favourable conditions for sensors. One way to reduce the risk of fake sensor data is to use multi-sensor consensus. This involves cross-referencing readings from multiple sensors to identify and discard any outliers or falsified data. Regular calibration and validation processes are also crucial to ensure sensor accuracy. Trusted hardware components or secure enclaves can provide an extra layer of security against tampering or unauthorized access, further enhancing the integrity and trustworthiness of sensor data.

X. CONCLUSION

IoT and blockchain can enhance supply chain security, transparency, and data visibility. We created a PoC that integrates IoT with blockchain to address supply chain challenges, illustrating the potential and advantages of allowing IoT devices to autonomously sign transactions to the blockchain using authenticated private keys, thus eliminating the need for external wallets.

Through the automation of transactions and integration of IoT devices, the PoC significantly enhances effectiveness, eliminates delays, and ensures real-time responsiveness. This approach confidently showcases IoT devices' secure communication and interaction with the blockchain network, allowing for continuous and automated transaction broadcasting. The detailed workflow of the use case and simulation results presented in this article make the research findings more accessible and showcase the practical implementation of the proposed method. This PoC demonstrates its suitability in scenarios where continuous, automated interaction with the blockchain is required through IoT devices.

REFERENCES

[1] M. C. Cooper, D. M. Lambert, and J. D. Pagh, "Supply chain management: More than a new name for logistics," *Int. J. Logistics Manag.*, vol. 8, no. 1, pp. 1–14, Jan. 1997.

[2] P. D. Larson and A. Halldorsson, "Logistics versus supply chain management: An international survey," *Int. J. Logistics Res. Appl.*, vol. 7, no. 1, pp. 17–31, Mar. 2004.

[3] V. Klapita, "Implementation of electronic data interchange as a method of communication between customers and transport company," *Transp. Res. Proc.*, vol. 53, pp. 174–179, Jan. 2021.

[4] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Comput. Ind. Eng.*, vol. 136, pp. 57–69, Oct. 2019.

[5] C. Bersani, "Safety in hazardous material road transportation: State of the art and emerging problems," *Advanced Technologies and Methodologies for Risk Management in the Global Transport of Dangerous Goods*, vol. 45. Sendai, Japan: IEEE, 2008, p. 88.

[6] F. Sahin and E. P. Robinson, "Flow coordination and information sharing in supply chains: Review, implications, and directions for future research," *Decis. Sci.*, vol. 33, no. 4, pp. 505–536, Sep. 2002.

[7] R. Alfalla-Luque, C. Medina-Lopez, and P. K. Dey, "Supply chain integration framework using literature review," *Prod. Planning Control*, vol. 24, nos. 8–9, pp. 800–817, 2013.

[8] A. Raja Santhi and P. Muthuswamy, "Influence of blockchain technology in manufacturing supply chain and logistics," *Logistics*, vol. 6, no. 1, p. 15, Feb. 2022.

[9] J. Browne, P. Sackett, and J. C. Wortmann, "Future manufacturing systems—Towards the extended enterprise," *Comput. Ind.*, vol. 25, no. 3, pp. 235–254, 1995.

[10] L. Ruiz-Garcia, P. Barreiro, and J. I. Robla, "Performance of ZigBee-based wireless sensor nodes for real-time monitoring of fruit logistics," *J. Food Eng.*, vol. 87, no. 3, pp. 405–415, Aug. 2008.

[11] V. Bordonaba-Juste and J. J. Cambra-Fierro, "Managing supply chain in the context of SMEs: A collaborative and customized partnership with the suppliers as the key for success," *Supply Chain Manag., Int. J.*, vol. 14, no. 5, pp. 393–402, Aug. 2009.

[12] A. A. Boschi, R. Borin, J. C. Raimundo, and A. Batocchio, "An exploration of blockchain technology in supply chain management," Tech. Rep., 2018.

[13] Y. Madhwal and P. Panfilov, "Blockchain and supply chain management: Aircrafts 'parts' business case," in *Proc. DAAAM*, 2017, pp. 1051–1056, doi: 10.2507/28th.daaam.proceedings.146.

[14] Z. Wenhua, F. Qamar, T.-A.-N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain technology: Security issues, healthcare applications, challenges and future trends," *Electronics*, vol. 12, no. 3, p. 546, Jan. 2023.

[15] L. Zhu, Y. Wu, K. Gai, and K.-K.-R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Gener. Comput. Syst.*, vol. 91, pp. 527–535, Feb. 2019.

[16] M. Turkanovic, M. Hölbl, K. Kosic, M. Hericko, and A. Kamicalic, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

[17] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[18] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions," *Wireless Netw.*, vol. 27, no. 1, pp. 55–90, Jan. 2021.

[19] X. Chen, C. He, Y. Chen, and Z. Xie, "Internet of Things (IoT)—Blockchain-enabled pharmaceutical supply chain resilience in the post-pandemic era," *Frontiers Eng. Manag.*, vol. 10, no. 1, pp. 82–95, 2023.

[20] I. Hasan, M. M. Habib, Z. Mohamed, and V. Tewari, "Integrated agri-food supply chain model: An application of IoT and blockchain," *Amer. J. Ind. Bus. Manag.*, vol. 13, no. 2, pp. 29–45, 2023.

[21] M. Oudani, A. Sebbar, K. Zkik, I. El Harraki, and A. Belhadi, "Green blockchain based IoT for secured supply chain of hazardous materials," *Comput. Ind. Eng.*, vol. 175, Jan. 2023, Art. no. 108814.

[22] A. Chandan, M. John, and V. Potdar, "Achieving UN SDGs in food supply chain using blockchain technology," *Sustainability*, vol. 15, no. 3, p. 2109, Jan. 2023.

[23] S. K. Nanda, S. K. Panda, and M. Dash, "Medical supply chain integrated with blockchain and IoT to track the logistics of medical products," *Multimedia Tools Appl.*, vol. 82, pp. 32917–32939, Mar. 2023.

[24] S. Popli, R. K. Jha, and S. Jain, "A survey on energy efficient narrowband Internet of Things (NBIoT): Architecture, application and challenges," *IEEE Access*, vol. 7, pp. 16739–16776, 2019.

[25] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[26] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in Ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.

[27] S. Seven, G. Yao, A. Soran, A. Onen, and S. M. Muyeen, "Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts," *IEEE Access*, vol. 8, pp. 175713–175726, 2020.

[28] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the Internet of Things supply chain management," *Sensors*, vol. 21, no. 5, p. 1759, Mar. 2021.

[29] Y. Khan, M. B. M. Su'ud, M. M. Alam, S. F. Ahmad, A. Y. B. Ahmad, and N. Khan, "Application of Internet of Things (IoT) in sustainable supply chain management," *Sustainability*, vol. 15, no. 1, p. 694, Dec. 2022.

[30] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "New blockchain-based architecture for service interoperations in Internet of Things," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 4, pp. 739–748, Aug. 2019.

[31] A. Babaei, M. Khedmati, M. R. A. Jokar, and E. B. Tirkolaee, "Designing an integrated blockchain-enabled supply chain network under uncertainty," *Sci. Rep.*, vol. 13, no. 1, p. 3928, Mar. 2023.

[32] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 122679–122695, 2022.

[33] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019, doi: 10.1109/tii.2019.2903342.

[34] P. Katsikouli, A. S. Wilde, N. Dragoni, and H. Høgh-Jensen, "On the benefits and challenges of blockchains for managing food supply chains," *J. Sci. Food Agricult.*, vol. 101, no. 6, pp. 2175–2181, 2021.

[35] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[36] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," *Comput. Ind.*, vol. 109, pp. 83–99, Aug. 2019.

[37] S. A. Bhat, N.-F. Huang, I. B. Sofi, and M. Sultan, "Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability," *Agriculture*, vol. 12, no. 1, p. 40, Dec. 2021.

[38] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet Things*, vols. 1–2, pp. 1–13, Sep. 2018.

[39] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227.

[40] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018, doi: 10.1109/mcom.2018.1800137.

[41] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, "Trustworthy IoT data streaming using blockchain and IPFS," *IEEE Access*, vol. 10, pp. 17707–17721, 2022, doi: 10.1109/access.2022.3149312.

[42] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, 2016.

[43] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A case study for blockchain in manufacturing: 'FabRec': A prototype for peer-to-peer network of manufacturing nodes," *Proc. Manuf.*, vol. 26, pp. 1180–1192, Jan. 2018.

[44] G. Papadodimas, G. Palaiokrasas, A. Litke, and T. Varvarigou, "Implementation of smart contracts for blockchain based IoT applications," in *Proc. 9th Int. Conf. Netw. Future (NOF)*, Nov. 2018, pp. 60–67, doi: 10.1109/nof.2018.8597718.

[45] B. B. Sezer, S. Topal, and U. Nuriyev, "TPPSUPPLY : A traceable and privacy-preserving blockchain system architecture for the supply chain," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103116.

[46] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, Oct. 2008.

[47] M. Iqbal and R. Matulevicius, "Exploring Sybil and double-spending risks in blockchain systems," *IEEE Access*, vol. 9, pp. 76153–76177, 2021.

[48] D. Korepanova, S. Kruglik, Y. Madhwal, T. Myaldzin, I. Prokhorov, I. Shiyanov, S. Vorobyov, and Y. Yanovich, "Blockchain-based solution to prevent postage stamps fraud," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrenc*, May 2019, pp. 171–175. [Online]. Available: https://ieeexplore.ieee.org/document/8751495/

[49] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, I. O. Ogu, and A. Zhavoronkov, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, Jan. 2018.

[50] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Comput. Ind. Eng.*, vol. 154, Apr. 2021, Art. no. 107130.

[51] V. Ermolaev, I. Klangberg, Y. Madhwal, S. Vapper, S. Wels, and Y. Yanovich, "Incorruptible auditing: Blockchain-powered graph database management," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency*, May 2020, pp. 101–103.

[52] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, Apr. 2019.

[53] O. Anyshchenko, I. Bohuslavskyi, S. Kruglik, Y. Madhwal, A. Ostrovsky, and Y. Yanovich, "Building cryptotokens based on permissioned blockchain framework," in *Proc. IEEE 90th Veh. Technol. Conf.*, Sep. 2019, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8891186/

[54] Y. Madhwal, Y. Borbon-Galvez, N. Etemadi, Y. Yanovich, and A. Creazza, "Proof of delivery smart contract for performance measurements," *IEEE Access*, vol. 10, pp. 69147–69159, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9804482/

[55] Z. Gao, D. Zhang, J. Zhang, L. Liu, D. Niyato, and V. C. M. Leung, "World state attack to blockchain based IoV and efficient protection with hybrid RSUs architecture," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 9952–9965, Sep. 2023.

[56] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[57] W. Metcalfe, "Ethereum, smart contracts, DApps," *Blockchain Crypt Currency*, vol. 77, pp. 77–93, Apr. 2020.

[58] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," Tech. Rep., 2015.

[59] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, CA, USA: O'Reilly Media, 2018.

[60] Y. Shahsavari, K. Zhang, and C. Talhi, "A theoretical model for block propagation analysis in Bitcoin network," *IEEE Trans. Eng. Manag.*, vol. 69, no. 4, pp. 1459–1476, Aug. 2022.

[61] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *Proc. IEEE P2P*, Sep. 2013, pp. 1–10.

[62] S. Li, L. Da Xu, and S. Zhao, "The Internet of Things: A survey," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 243–259, Apr. 2015.

[63] Y. Jeong, H. Joo, G. Hong, D. Shin, and S. Lee, "AVIoT: Web-based interactive authoring and visualization of indoor Internet of Things," *IEEE Trans. Consum. Electron.*, vol. 61, no. 3, pp. 295–301, Aug. 2015.

[64] B. Gross and N. Dierksheide, "Power systems," vol. 3, no. 2, pp. 368–374, 2012.

[65] J.-P.-A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess. Microsyst.*, vol. 77, Sep. 2020, Art. no. 103201.

[66] N. Kozodoi, J. Jacob, and S. Lessmann, "Fairness in credit scoring: Assessment, implementation and profit implications," *Eur. J. Oper. Res.*, vol. 297, no. 3, pp. 1083–1094, Mar. 2022.

[67] S. Kaiser, M. S. Haq, A. S. Tosun, and T. Korkmaz, "Container technologies for arm architecture: A comprehensive survey of the state-of-the-art," *IEEE Access*, vol. 10, pp. 84853–84881, 2022.

[68] P. Gupta. Accessed: Jun. 2023. [Online]. Available: https://www.educba.com/what-is-arduino-uno/

[69] A. Sanjeev. (Mar. 2018). [Online]. Available: https://maker.pro/raspberry-pi/tutorial/how-to-connect-and-interface-raspberry-pi-with-arduino

[70] R. P. Foundation. *Physical Computing With Python*. Accessed: Jun. 2023. [Online]. Available: https://projects.raspberrypi.org/en/projects/physical-computing/13

[71] P. Murugesan. (2022). *What is.env? How to Set up and Run a.env File in Node?* [Online]. Available: https://www.codementor.io/@parthibakumarmurugesan/what-is-env-how-to-set-up-and-run-a-env-file-in-node-1pnyxw9yxj

[72] ConsenSys. *Metamask Chrome Extension*. Accessed: Jun. 2023. [Online]. Available: https://metamask.io/

[73] J. Howell. (Aug. 2022). *Hardhat vs Truffle—Key Diffe*. [Online]. Available: https://101blockchains.com/hardhat-vs-truffle/

[74] *Blockchain Explorer*. Accessed: Jun. 2023. [Online]. Available: https://www.blockchain.com/explorer

[75] P. Psenák and M. Tibenský, "The usage of Vue JS framework for Web application creation," *Mesterséges Intelligencia*, vol. 2, no. 2, pp. 61–72, 2020.

[76] L. Rosencrance. (2022). *Remote Procedure Call (RPC)*. [Online]. Available: https://www.techtarget.com/searchapparchitecture/definition/Remote-Procedure-Call-RPC

[77] Y. Madhwal. (2023). *A Proof-of-Concept for IoT Device Integration With Blockchain*. [Online]. Available: https://github.com/yashmadhwal/IoT_Blockchain_SCM/

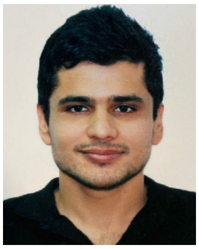
[78] S. Mason. (2023). *Does Cream Cheese Need to be Refrigerated*. [Online]. Available: https://eatpallet.com/does-cream-cheese-need-to-be-refrigerated/

[79] CargoHandbook. *Cheese*. Accessed: Jun. 2023. [Online]. Available: https://cargohandbook.com/Cheese

[80] *Cheese Production in the us*. Accessed: Jun. 2023. [Online]. Available: https://www.ibisworld.com/industry-statistics/number-of-businesses/cheese-production-united-states/

[81] W. Tang. (2019). *EIP-2200: Structured Definitions for Net Gas Metering*. [Online]. Available: https://eips.ethereum.org/EIPS/eip-2200

[82] P. Kostyuk, S. Kudryashov, Y. Madhwal, I. Maslov, V. Tkachenko, and Y. Yanovich, "Blockchain-based solution to prevent plastic pipes fraud," in *Proc. 7th Int. Conf. Softw. Defined Syst. (SDS)*, Apr. 2020, pp. 208–213, doi: 10.1109/sds49854.2020.9143879.



YASH MADHWAL (Member, IEEE) is a Research Scientist with the Skolkovo Institue of Science and Technology (Skoltech), specializing in implementing blockchain technology in resolving supply chain problems. He is also a teaching assistant of the course "Introduction to Blockchain" and conducts technical seminars, showing the listeners methods to build blockchain applications. Additionally, he is a guest lecturer with different universities to deliver an introductory lecture on blockchain technology and its potential applications. He has authored multiple scientific papers, where he has built prototypes of the blockchain-based decentralized application (DApp), focusing on industrial problems, especially the supply chain.

YURY YANOVICH (Member, IEEE) received the bachelor's and master's degrees (Hons.) in applied physics and mathematics from the Moscow Institute of Physics and Technology, Moscow, Russia, in 2010 and 2012, respectively, and the Ph.D. degree in probability theory and mathematical statistics from the Institute for Information Transmission Problems, Moscow, in 2017.

He is a Senior Research Scientist with the Skolkovo Institute of Science and Technology, Moscow. He has been a lecturer of the "Introduction to Blockchain" course with top Russian universities, since 2017. He is the author of Exonum consensus protocol. His research interests include blockchain, consensus protocols, privacy, and applications.

S. BALACHANDER received the M.S. degree from the School of Information Technology, Vellore Institute of Technology, Vellore, India. He is currently pursuing the Ph.D. degree in blockchain technology with the School of Data Science and Business Systems, SRM Institute of Science and Technology. His research interests include blockchain technology, information security, and cryptography.

K. HARSHINI POOJAA received the M.Tech. degree from the School of Information Technology, Vellore Institute of Technology, Vellore, India, in 2018. She is currently pursuing the Ph.D. degree with the Department of Data Science and Business System, SRM Institute of Science and Technology, Chengalpattu, India. She is also a Assistant Professor with the Department of Data Science and Business System, SRM Institute of Science and Technology. Her research interests include blockchain, cryptography, scalability, and privacy protection.

R. SARANYA received the M.E. degree from the Department of Computer Science and Engineering, KCG College of Technology, affiliated to Anna University, Chennai, India, in 2015. She is currently pursuing the Ph.D. degree with the Department of Data Science and Business Systems, SRM Institute of Science and Technology, Chennai. She has presented research papers at international and national conferences and published one Indian patent. Her research interests include blockchain technology, cloud computing, big data analytics, and data mining.

B. SUBASHINI received the bachelor's degree in information technology from PSG Tech Coimbatore and the master's degree in information technology and computer science from Anna University and SRM University. She is an Assistant Professor with the Data Science and Business Systems Department, SRM Institute of Science and Technology, Chengalpattu, India. She possesses more than ten years of teaching experience. Her research incorporates blockchain technology to address traceability concerns in the agro-food supply chain. Her areas of interests include database management systems, supply chain management, the IoT, web technology, information security, network security, cryptography, and blockchain technology.